Sentinel 7.3 Release Notes

February 2015



Sentinel 7.3 includes new features, improves usability, and resolves several previous issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Sentinel forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Sentinel NetIQ Documentation page. To download this product, see the Sentinel Product Upgrade website.

1 What’s New?

The following sections outline the key features and enhancements, and also the issues resolved in this release:

1.1 Single Unified Platform for Sentinel and Sentinel Log Manager

NetIQ now delivers Sentinel as a single platform for both Sentinel and Sentinel Log Manager solutions.

The Sentinel platform provides two main solutions:

* **Sentinel Enterprise:** A full-featured solution that enables real-time security analytics and many additional features. Sentinel Enterprise focuses on SIEM use cases such as real-time threat detection, alerting, and remediation.
* **Sentinel for Log Management:** A solution for log management use cases such as the ability to collect, store, search, and report on data.

NetIQ provides separate licenses for each of these solutions. For new installations, the Sentinel platform enables the functionality depending on whether you enter a Sentinel Enterprise or Sentinel for Log Management license key. There is no impact of this change on existing Sentinel servers or upgrades.

For more information about the features enabled in each solution, see "Understanding License Information " in the *NetIQ Installation and Configuration Guide.*

1.2 Alert Notifications and Triage

You can now configure correlation rules to receive instant alert notification about any potential threats. Alerts notify you of what is most important for you to look at. Alerts can relate to threats to IT resources or performance thresholds, such as system memory full or IT resources not responding. Sentinel automatically associates the relevant events and identities with the alert to help you determine the root cause of potential threat.

For more information, see "Configuring Alert Notifications" in the *NetIQ Sentinel Administration Guide*.

Sentinel provides a graphical and tabular representation of alerts in real-time alert views. You can perform alert triage operations, changing states of an alert, assigning alerts to users or roles, adding information to the knowledge base, and so on. You can further drill-down into each alert to view the alert details, such as trigger events, user identities involved, and alert history. For more information about alert view, see "Viewing and Triaging Alerts in Alert Views" in the "*NetIQ Sentinel User Guide.*"

1.3 Alert Dashboards

Alert dashboards enable you to perform powerful exploration and analysis of alerts. The Alert dashboard provides an easy-to-configure, customizable interface that helps you to view and investigate alerts in detail. For example, you can find out the average time taken by owners to close alerts, the correlation rule generating the maximum number of alerts, average number of consolidated alerts, geographical locations of alerts with high severity, and so on. For more information about alert dashboards, see "Analyzing Alert Dashboards" in the "*NetIQ Sentinel User Guide.*"

1.4 Real-Time Event Views in the Web Interface

You can now view events in real-time in the Sentinel Web Interface without having to log in to Sentinel Control Center. Real-time event views provide summarized event data. To view the event details or perform any event operations, you can use the Search interface. For more information about viewing real-time event views in the Web Interface, see "Viewing Events in the Web Interface" in the *NetIQ Sentinel User Guide*.

1.5 Plug-Ins Catalog

You can now view the list of plug-ins installed in the Sentinel server. The **Plug-ins** > **Catalog** interface lists all Collectors, Connectors, Actions, Integrators, and Feeds installed in your Sentinel server. You can also see the version, release date, and other metadata of a plug-in, which helps you determine whether you have the latest version of a plug-in. To view the list of plug-ins, you must be in the administrator role.

1.6 Appliance in OVF Format

Sentinel now provides appliance in Open Virtual Machine (OVF) format, which eliminates the need for different appliance formats for each virtualization software. The Sentinel OVF appliance replaces the VMware and Xen appliances. You can use the OVF appliance to install Sentinel on VMware and Citrix Xen virtualization platforms. The appliance updates in the NCC channel will continue to update existing appliances in the Xen or VMware formats. For more information about installing the Sentinel appliance in OVF format, see "Installing OVF Appliance" in the *NetIQ Sentinel Installation and Configuration Guide*.

1.7 Enhancements to Multi-Tenancy Configuration

Sentinel 7.3 provides several enhancements to support multi-tenancy configuration for Managed Security Service Providers (MSSPs):

- **Ability to manage tenants:** A new user interface is available that enables you to create tenants in advance of receiving any data from that tenant. The user interface also provides the ability to enable and disable tenants.
- **Tenant-specific roles and users:** When creating roles, you can now assign a role to the default tenant or a specific tenant. The default tenant provides access to data for all tenants. You can use the default tenant in environments without tenants and for MSSP users who require access to data from all tenants. Users in a role assigned to a specific tenant can view only the data tagged with that tenant name. MSSP employees who need to view multiple tenants' data can be assigned to the default tenant, which gives them access to data and real-time views of all tenants.

For detailed information about these enhancements and to configure multi-tenancy, see "Configuring Sentinel in Multi-Tenancy Environments" in the *NetIQ Sentinel Administration Guide*.

1.8 Enhancements to Correlated Events

Sentinel 7.3 includes the following enhancements to correlated events:

- **Ability to customize the correlated event:** The **Correlation** interface now includes an option that enables you to customize the correlated event field values when creating the correlation rule. For example, if you want a correlated event to have a different severity than its trigger events, you can set the Severity to a new value. For more information, see "Customizing Correlated Event" in the *NetIQ Sentinel User Guide*.

- **Ability to configure the number of trigger events:** You can now define the number of trigger events that can be associated to a correlation rule. Defining this limit prevents Sentinel from associating a large number of trigger events to the correlated event, thereby reducing the load on the server. For more information, see "Configuring the Number of Trigger Events to Associate with a Correlated Event"in the *NetIQ Sentinel Administration Guide*.

1.9 Enhancements in Security Intelligence Dashboards

Sentinel 7.3 includes the following enhancements in Security Intelligence dashboards:

- **Ability to include historical data:** You can now include historical data when populating the security intelligence data in the dashboard, which provides more context when analyzing the data.
- **More data retention periods:** You can now retain the security intelligence data up to 64 weeks.

For more information, see "Creating a Dashboard" in the *NetIQ Sentinel User Guide*.

1.10 Terminology Changes for Multi-Instance (Distributed) Setup

Sentinel 7.3 changes the terminology used in the multi-instance (distributed) setup user interface. These changes reflect that the multi-instance setup is intended for data federation and is not specific to just search or events. The terminology changes are as follows:

- Distributed Search is now Data Federation
- Targets is now data sources
- Search target server is now data source server
- Search initiator server is now authorized requestor

For more information, see "Configuring Data Federation" in the *NetIQ Sentinel Administration Guide*.

1.11 Enhancements to Sentinel Licensing

The default trial license for a new installation of Sentinel allows you to use all the features of Sentinel Enterprise for an evaluation period of 60 days with unlimited EPS. After the trial license expires the system runs with a free license key that enables a limited set of features and a limited event rate of 25 EPS. The free license never expires. For more information about Sentinel licenses, see "Understanding License Information "in the *NetIQ Installation and Configuration Guide.*

1.12 Ability to Resize the Dynamic List Properties Window

You can now resize the Dynamic List Properties window, which makes it easier to view long values.

1.13 Auto-Deletion of Old Reports

Sentinel automatically deletes old reports to optimize the usage of disk space. You can define the report retention period as desired. For more information, see "Configuring the Report Retention Period" in the *NetIQ Sentinel Administration Guide*.

1.14 Latest Plug-Ins

Sentinel 7.3 includes new and updated versions of Sentinel plug-ins. The latest version of Collectors and Connectors are available only when you perform a new installation. The latest versions of Integrators and Actions are available in both new and upgrade installations. For upgrade installations of Sentinel 7.3, you can visit the Sentinel Plug-ins website, review the revision history of the latest Collectors and Connectors in the specific documentation, and then determine which plug-ins to download and install.

1.15 Software Fixes

Sentinel 7.3 includes software fixes that resolve several issues.

For the list of software fixes and enhancements in previous releases, see the specific release notes.

1.15.1 Cannot Export Distributed Search Results with More Than 50,000 Events

Issue: You cannot export distributed search results with more than 50,000 events to a file. `(BUG 863985)`

Fix: You can now export search result files containing up to 200,000 events.

1.15.2 Raw Data Buffer Size Has a Set Limit to Store Incoming Data

Issue: The raw data buffer has a set limit to store incoming raw data. If the incoming data exceeds the limit, Sentinel discards the raw data even when there is sufficient disk space. `(BUG 893546)`

Fix: There is no limit on the raw data buffer size. Sentinel can buffer raw data until the disk space is 90% full.

1.15.3 Cannot Redeploy a Correlation Rule If Multiple Rule Tabs are Open

Issue: Cannot redeploy correlation rules if more than one rule tab is open at the same time. (BUG 838771)

Fix: You can now redeploy correlation rules when multiple rule tabs are open at the same time.

1.15.4 Need to Press the Enter Key Twice When Doing an Event Search

Issue: When doing an event search, if you edit the search query, you need to press Enter or **Search** twice for the search to begin.(BUG 829291)

Fix: Event search begins when you press Enter or **Search** once after editing a search query.

1.15.5 Cannot View Change Guardian Event Details Without the Change Guardian License Key

Issue: Sentinel prompts for the Change Guardian license when you click the Change Guardian icon to view event details. (BUG 855914)

Fix: You now view the Change Guardian event details without adding the Change Guardian license key.

1.15.6 Appliance Upgrade Installer Deletes Custom Firewall Rules During the Upgrade

Issue: Sentinel deletes existing custom firewall rules during Sentinel appliances upgrade. (BUG 867662)

Fix: Sentinel 7.3 preserves the existing custom firewall rules.

1.15.7 Errors When Processing Raw Data

Issue: Sentinel does not process raw data files that were not closed properly. This is a sporadic issue.(BUG 870969)

Fix: Sentinel 7.3 now processes the raw data files that were not closed properly.

1.15.8 Attribute Filter in the Event Source Management View Does Not Automatically Expand Event Sources

Issue: In the Event Source Management table view, filtering by attributes presents a collapsed view of the event sources. You need to expand the view manually. (BUG 790041)

Fix: In Sentinel 7.3, the Event Source Management view expands automatically when you filter by attributes.

1.15.9 Sentinel Does Not Display the Change Guardian Event Attachments After One View

Issue: Sentinel does not display the Change Guardian event attachments after you view the attachments once. It displays the event attachments correctly only for the first time. (BUG 902142)

Fix: Sentinel 7.3 displays the Change Guardian event attachments correctly.

1.15.10 Database Synchronization Between Sentinel and Sentinel Agent Manager Does Not Happen Reliably

Issue: Activities that you do in Sentinel Agent Manager (SAM), such as authorizing an agent, are not always synchronized to Sentinel. This issue occurs because of an error in the ETL script used to synchronize the SAM database and the Sentinel database. `(BUG 885456)`

Fix: In Sentinel 7.3, synchronization between the SAM database and the Sentinel database happens correctly. Tasks performed in SAM are synchronized to Sentinel within a few minutes.

1.15.11 Geospatial Event Fields Are Not Populated With the Correct Data

Issue: The Latitude, Longitude, and Country geospatial event fields for Source, Target, and Observer host are set incorrectly. `(BUG 895872)`

Fix: Sentinel now populates the Latitude and Longitude event fields with correct values. The Country event fields are now populated with the two character ISO country code instead of the full country name, so that they are compatible with more locales and visualization tools.

1.15.12 The clean_db.sh Script Does Not Delete Advisor Data in Custom Installations

Issue: The `clean_db.sh` script does not delete Advisor data in custom installations, where Advisor data is present in non-default locations. `(BUG 820700)`

Fix: The `clean_db.sh` script now deletes Advisor data from both default and non-default locations.

1.15.13 Connection Problems Between Clients and Sentinel Running in FIPS Mode

Issue: Previous versions of Sentinel include Oracle Java 1.7 update 65, which has a known issue related to RSA client key exchange in FIPS mode. For more information, see the Java SE Development Kit 7, Update 51 Release Notes. This causes connection problems when Sentinel is running in FIPS mode and attempting to receive connections from clients such as Security Manager and Sentinel Agent Manager. `(BUG 872305)`

Fix: Sentinel 7.3 includes Oracle Java 1.7 update 72, which resolves the RSA key exchange issue.

1.15.14 Event Search Does Not Work After a Failed Distributed Search

Issue: Sentinel does not return any results when you perform an event search after a failed distributed search. Event search stops working, and it does not allow you to perform any new search. `(BUG 864372)`

Fix: Sentinel now closes the search jobs that are waiting for data after a failed search, and allows new searches.

2 System Requirements

For information about hardware requirements, supported operating systems, and browsers, see “Meeting System requirements” in the *NetIQ Sentinel Installation and Configuration Guide*.

3 Installing Sentinel 7.3

For information about installing Sentinel 7.3, see the *NetIQ Sentinel Installation and Configuration Guide*.

4 Upgrading to Sentinel 7.3

You can upgrade to Sentinel 7.3 from Sentinel 7.0 or later.

Download the Sentinel installer from the NetIQ Download website. For information about upgrading to Sentinel 7.3, see "Upgrading Sentinel" in the *NetIQ Sentinel Installation and Configuration Guide*.

4.1 Post Upgrade Configuration

After the upgrade, the Data Proxy User role will not have the **Allow users to manage alerts** permission. This permission is necessary for the role to be able to perform remote alert search. Assign the **Allow users to manage alerts** permission to the Data Proxy User role Manually. For more information, see "Configuring Roles and Users" in the *NetIQ Sentinel Administration Guide*.

5 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

5.1 Tips Table Search Does Not Return the Complete List of Alert Fields in Upgraded Sentinel Installations

Issue: In upgraded installations of Sentinel 7.3, when you search for alert attributes in the Tips table in the Web Console, the search does not return the complete list of alert fields. However, alert fields display correctly in the Tips table if you clear the search. `(BUG 914755)`

Workaround: There is no workaround at this time.

5.2 Cannot Launch Sentinel Control Center and Solution Designer Using JRE 8 When Sentinel is in FIPS Mode

Issue: When the Sentinel server is running in FIPS 140-2 mode, you cannot launch Sentinel Control Center and Solution Designer in the client computer using Java Web Start if the Java Runtime Environment (JRE) version is 8 or later. `(BUG 910452)`

Workaround: Ensure that you perform the following in the client computer where you want to launch Sentinel Control Center or Solution Designer:

- Install and use JRE 7 to launch Sentinel Control Center or Solution Designer.
- In the Java Control Panel, do not select the **Use TLS 1.2** option in the **Advanced** tab.

5.3 Data Synchronization Fails While Synchronizing IPv6 Addresses in Human Readable Format

Issue: Data synchronization fails when you try to synchronize IPv6 address fields in a human readable format to external databases. For information about configuring Sentinel to populate the IP address fields in human readable dot notation format, see "Creating a Data Synchronization Policy" in *NetIQ Sentinel Administration Guide*. `(BUG 913014)`

Workaround: To fix this issue, manually change the maximum size of the IP address fields to at least 46 characters in the target database, and re-synchronize the database.

5.4 Event Search Does Not Respond if You Do Not Have Any Event Viewing Permissions

Issue: If run an event search when your role's security filter is blank and your role does not have event viewing permissions, the search does not complete. The search does not display any error message about the invalid event viewing permissions. `(BUG 908666)`

Workaround: Update the role with one of the following options:

1. Specify a criteria in the **Only events matching the criteria** field. If users in the role should not see any events, you can enter **NOT sev:[0 TO 5]**.
2. Select **View system events**.
3. Select **View all event data (including raw data and NetFlow data)**.

5.5 Sentinel Agent Manager Does Not Consider the RawDataTapFileSize Configuration

Issue: Sentinel Agent Manager ignores the value specified in `RawDataTapFileSize` attribute in the `SMServiceHost.exe.config` file for the raw data file size configuration, and stops writing to the raw data file when the file size reaches 10 MB. `(BUG 867954)`

Workaround: Manually copy the content of the raw data file into another file and clear it when the file size reaches 10 MB, so that Sentinel Agent Manager can write new data into it.

5.6 The Event fields Panel is Missing in the Schedule Page When Editing Some Saved Searches

Issue: When editing a saved search upgraded from Sentinel 7.2 to a later version, the **Event fields** panel, used to specify output fields in the search report CSV, is missing in the schedule page. `(BUG 900293)`

Workaround: After upgrading Sentinel, recreate and reschedule the search to view the **Event fields** panel in the schedule page.

5.7 Sentinel Does Not Return Any Correlated Events When You Search for Events for the Deployed Rule with the Default Fire Count Search

Issue: Sentinel does not return any correlated events when you search for all correlated events that were generated after the rule was deployed or enabled, by clicking the icon next to **Fire count** in the **Activity statistics** panel in the Correlation Summary page for the rule. `(BUG 912820)`

Workaround: Change the value in the **From** field in the Event Search page to a time earlier than the populated time in the field and click **Search** again.

5.8 Sentinel in FIPS Mode Does Not Display Change Guardian Delta Attached information

Issue: Sentinel running in FIPS mode does not display Change Guardian delta attached information when you search for Change Guardian events and click the **Change Guardian** icon, in spite of being configured to receive Change Guardian events. Change Guardian 4.1.1.1 and earlier versions do not support sending events in FIPS-compatible mode. `(BUG 912230)`

Workaround: There is no workaround at this time.

5.9 Occurrences Count Decreases After Refreshing the Alert View

Issue: In the alert view, the **Occurrences** count decreases when you refresh the alert view. `(BUG 913838)`

Workaround: Navigate to the alert summary page by clicking **View details** next to the alert for which the **Occurrences** count has decreased. The alert summary page displays the correct **Occurrences** value.

5.10 Data Collection and Data Synchronization With the DB2 Database Fail After Upgrading to Sentinel 7.3

Issue: Upgrading to Sentinel 7.3 causes data collection and data synchronization with the DB2 database to fail, because the upgrade removes the IBM DB2 JDBC driver. (BUG 909343)

Workaround: After upgrading to Sentinel 7.3, add the correct JDBC Driver and configure it for data collection and data synchronization, by performing the following steps:

1. Copy the correct version of the IBM DB2 JDBC driver (`db2jcc-*.jar`) for your version of the DB2 database in the `/opt/novell/sentinel/lib` folder.
2. Ensure that you set the necessary ownership and permissions for the driver file.
3. Configure this driver for data collection. For more information, see the Database Connector documentation.

5.11 New Incoming Alerts Incorrectly Appear to be Selected When You Modify Existing Alerts

Issue: When you click **Select All** in alerts views to select alerts, deselect few alerts, and modify them, new incoming alerts are also selected in the refreshed alert views. This results in wrong count of alerts selected for modification, and also it appears as if you are modifying new incoming alerts too. However, only the originally selected alerts are modified. (BUG 904830)

Workaround: No new alerts will appear in the alert view if you create the alert view with a custom time range.

5.12 Loading Historical Security Intelligence Data Takes a Long Time

Issue: Historical Security Intelligence (SI) data takes a long time to load in Sentinel systems that have a high Events Per Second (EPS) load. (BUG 908599)

Workaround: If you are creating a security intelligence dashboard with historical data, plan to deploy the dashboard when the load on your system is lower, if possible. There is no other workaround at this time.

5.13 Security Intelligence Dashboard Displays Invalid Baseline Duration When Regenerating a Baseline

Issue: During Security Intelligence baseline regeneration, the start and finish dates for the baseline are incorrect and display 1/1/1970. (BUG 912009)

Workaround: The correct dates are updated after the baseline regeneration is complete.

5.14 Sentinel Server Shuts Down When Running a Search If There Are Large Number of Events in a Single Partition

Issue: Sentinel server shuts down when you run a search if there are a large number of events indexed in a single partition. (BUG 913599)

Workaround: Create retention policies in such a way that there are at least two partitions open in a day. Having more than one partition open helps reduce the number of events indexed in partitions.

You can create retention policies that filter events based on the `estzhour` field, which tracks the hour of the day. Therefore, you can create one retention policy with `estzhour:[0 TO 11]` as the filter and another retention policy with `estzhour:[12 TO 23]` as the filter.

For more information, see "Configuring Data Retention Policies" in the *NetIQ Sentinel Administration Guide*.

5.15 Alert Roll-Up Occasionally Fails and New Alert is Created

Issue: A new alert is created instead of alert information rolling up to an existing alert. This is a sporadic issue. `(BUG 914512)`

Workaround: There is no workaround at this time.

5.16 Error While Using the report_dev_setup.sh Script to Configure Sentinel Ports for Firewall Exceptions on Upgraded Sentinel Appliance Installations

Issue: Sentinel displays an error when you use the `report_dev_setup.sh` script to configure Sentinel ports for firewall exceptions. `(BUG 914874)`

Workaround: Configure Sentinel ports for firewall exceptions through the following steps:

1. Open the `/etc/sysconfig/SuSEfirewall2` file.
2. Change the following line:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   to

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Restart Sentinel.

5.17 Sentinel Generic Collector Performance Degrades When Generic Hostname Resolution Service Collector is Enabled

Issue: Sentinel Generic Collector performance degrades when Generic Hostname Resolution Service Collector is enabled on Microsoft Active Directory and Windows Collector. EPS decreases by 50% when remote Collector Managers send events. `(BUG 906715)`

Workaround: There is no workaround at this time.

5.18 Sentinel Cannot Access Security Intelligence, Netflow, and Alert Data in FIPS Mode

Issue: When you install Sentinel in FIPS mode, connector to Security Intelligence database fails to start, and Sentinel cannot access Security Intelligence, Netflow, and alert data. `(BUG 915241)`

Workaround: Restart Sentinel after installing and configuring in FIPS mode.

5.19 Security Intelligence Database and Alert Dashboard Occasionally Do Not Work in Upgraded Custom Installations of FIPS Enabled Sentinel

Issue: When you upgrade to Sentinel 7.3 from a custom installation of Sentinel that was installed by a non-root user and was configured in FIPS mode, Security Intelligence database and Alert Dashboard occasionally do not start. (BUG 916285)

Workaround: Perform the following steps:

1. Go to <*custom installation directory*>/opt/novell/sentinel/bin to know the Sentinel Indexing Service.
2. Run the following command:

   ```
   ./si_db.sh status
   ```

   Verify whether the following output displayed:

   ```
   Connection between alert store and indexing service is running.
   Security Intelligence database is running.
   Indexing service is running.
   ```

   If any of the above mentioned three services are not running, perform the following steps.
3. Run the following command to stop Sentinel:

   ```
   rcsentinel stop
   ```
4. Log in to the Sentinel server as the novell user.
5. Run the following command:

   ```
   <custom installation directory>/opt/novell/sentinel/bin/si_db.sh startnoauth
   ```
6. Run the following commands to add dbauser and appuser users:

   ```
   cd <custom installation directory>/opt/novell/sentinel/3rdparty/mongodb/bin
   ./mongo
   use admin
   db.addUser ("dbauser", "novell")
   use analytics
   db.addUser ("appuser", "novell")
   exit
   ```
7. Run the following command:

   ```
   <custom installation directory>/opt/novell/sentinel/bin/si_db.sh stop
   ```
8. Perform the following steps to add encrypted password fields:

   8a Run the following command to get the encrypted password for the novell user:

   ```
   <custom installation directory>/opt/novell/sentinel/bin/encryptpwd -e
   novell
   ```

   Encrypted password is displayed. For example:

   ```
   bVWOzu6okMmMCkgM0aHeQ==
   ```

   8b In the configuration.properties file, update the baselining.sidb.password and baselining.sidb.dbpassword properties with the encrypted

   password. for example:

```
baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==
baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==
```

9 Exit from novell user account and start Sentinel as root user using the following command:

```
rcsentinel start
```

NOTE: Run the `configure.sh` script to reset the password whenever needed. For more information about running the `configure.sh` script, see "Modifying the Configuration after Installation" in the *NetIQ Sentinel Installation and Configuration Guide*.

5.20 Sentinel Does Not Display Trigger Events for Remote Alerts

Issue: In alert views, when you click **View Details** next to any remote alert and go to the Alert Details page, trigger events for that alert do not display in the **Associated Data** panel. (BUG 916116)

Workaround: Log in to the data source server and view the alert details locally.

5.21 Sentinel Does Not Display Customized Alert Properties in Alert Views for Remote Alerts

Issue: In alert views, **State** and **Priority** fields remote alerts display no data if the values for these fields are customized. These fields display no data in Alert Details page for the alerts too. (BUG 915762)

Workaround: Log in to the data source server and view the alerts locally.

5.22 Sometimes Sentinel Does Not Display Alerts in Alert Views After a Restart

Issue: Sometimes, Sentinel does not display alerts in any alert view if you restart Sentinel and log in. (BUG 916133)

Workaround: Restart the Security Intelligence database by performing the following steps:

1 Run the following command:

```
rm /opt/novell/sentinel/3rdparty/mongoconnector/config.txt
```

2 Edit `/opt/novell/sentinel/bin/elasticsearch.sh` as follows:

2a Enter the following after line number 209:

```
sleep 2
```

2b Save the file and exit the editor.

3 Run the following command as novell user:

```
/opt/novell/sentinel/bin/si_db.sh restart
```

5.23 Users Missing in Security Intelligence Database in Upgraded Sentinel Appliance Installations

Issue: In the upgraded Sentinel appliance online installations, appuser and dbauser user accounts are not available. (BUG 915197)

Workaround: Perform the following steps:

1 Run the following command:

```
/opt/novell/sentinel/bin/si_db.sh startnoauth
```

2 Run the following commands to add dbauser and appuser users:

```
cd opt/novell/sentinel/3rdparty/mongodb/bin
./mongo
use admin
db.addUser ("dbauser", "novell")
use analytics
db.addUser ("appuser", "novell")
exit
```

3 Run the following command:

```
/opt/novell/sentinel/bin/si_db.sh stop
```

4 Perform the following steps to add encrypted password fields:

4a Run the following command to get the encrypted password for the novell user:

```
/opt/novell/sentinel/bin/encryptpwd -e novell
```

Encrypted password is displayed. For example:

```
bVWOzu6okMmMCkgM0aHeQ==
```

4b In the `configuration.properties` file, update the `baselining.sidb.password` and `baselining.sidb.dbpassword` properties with the encrypted

password. for example:

```
baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==
baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==
```

5 Exit from novell user account and start Sentinel as root user using the following command:

```
rcsentinel start
```

5.24 Sentinel Does Not Configure the Sentinel Appliance Network Interface By Default

Issue: When installing Sentinel Appliance, the network interface is not configured by default. `(BUG 867013)`

Workaround: To configure the network Interface:

1 In the Network Configuration page, click **Network Interfaces**.
2 Select the network interface and click **Edit**.
3 Select **Dynamic Address** and then select either **DHCP** or **Static assigned IP Address**.
4 Click **Next** and then **OK**.

5.25 The Web Browser Displays an Error When Exporting Search Results in Sentinel

Issue: When exporting search results in Sentinel, the Web browser might display an error if you modify the operating system language settings. `(BUG 834874)`

Workaround: To export search results properly, perform either of the following:

- While exporting the search results, remove any special characters (outside the ASCII characters) from the export filename.
- Enable UTF-8 in the operating system language settings, restart the machine, and then restart the Sentinel server.

5.26 Launching the Sentinel Web Console with Port Forwarding or Destination Network Address Translation Displays a Blank Page

Issue: When you launch the Sentinel Web Console using port forwarding or Destination Network Address Translation (DNAT), Sentinel Web Console displays a blank page. `(BUG 694732)`

Workaround: Do not use port forwarding or Destination Network Address Translation (DNAT) to launch the Sentinel Web Console.

5.27 Sentinel Might Display an Error When You Create or Regenerate a Baseline

Issue: When you create or regenerate a security intelligence baseline, Sentinel creates the baseline successfully, but displays an error message. `(BUG 848067)`

Workaround: Ignore the error message. The creation of the baseline may take several minutes.

5.28 Partitions Removed from Secondary Storage are Also Removed from Primary Storage

Issue: If the number of days of data that secondary storage can hold is less than the number of days of data that primary storage holds, Sentinel does not use the disk space in primary storage efficiently. Partitions removed from secondary storage to free up space will also be removed from primary storage. `(BUG 860888)`

Workaround: Allocate enough space in secondary storage to hold data for the total number of days you want to keep online (searchable).

For more information, see “Event Data” in the *NetIQ Sentinel Administration Guide*.

5.29 Sentinel Services Might Not Start Automatically After the Installation

Issue: On systems with more than 2 TB disk space, Sentinel might not start automatically after the installation. `(BUG 846296)`

Workaround: As a one-time activity, start the Sentinel services manually by specifying the following command:

```
rcsentinel start
```

5.30 Cannot Enable Kerberos Authentication in Sentinel Appliance Installations

Issue: In Sentinel appliance installations, if you configure Kerberos authentication in the Kerberos module, the console displays a confirmation message that the Kerberos client configuration was successful. When you view the Kerberos module again, however, the **Enable Kerberos Authentication** option is deselected. `(BUG 843623)`

Workaround: There is no workaround at this time.

5.31 Unable to Install the Remote Collector Manager If the Password Contains Special Characters

Issue: When you install a remote Collector Manager, if you specify a password that contains special characters, such as '$', '"', '\', or '/', the installation fails with errors. `(BUG 812111)`

Workaround: Do not use special characters in the remote Collector Manager password.

5.32 Restarting a Remote Collector Manager Causes Some Event Sources to Lose Connection

Issue: When you restart a remote Collector Manager appliance, the Syslog event sources connected on the UDP port lose connection. `(BUG 795057)`

Workaround: There is no workaround available at this time.

5.33 Unable to View More Than One Report Result at a Time

Issue: While you wait for one report result PDF to open, particularly report results of 1 million events, if you click another report result PDF to view, the report result is not displayed. `(BUG 804683)`

Workaround: Click the second report result PDF again to view the report result.

5.34 Agent Manager Requires SQL Authentication When FIPS Mode is Enabled

Issue: When FIPS mode is enabled in your Sentinel environment, using Windows authentication for Agent Manager causes synchronization with the Agent Manager database to fail. `(BUG 814452)`

Workaround: Use SQL authentication for Agent Manager when FIPS mode is enabled in your Sentinel environment.

5.35 Sentinel High Availability Installation in FIPS Mode Displays an Error

Issue: If FIPS mode is enabled, the Sentinel High Availability installation displays the following error:

```
Sentinel server configuration.properties file is not correct. Check the
configuration file and then run the convert_to_fips.sh script again to enable FIPS
mode in Sentinel server.
```

However, the installation completes successfully. `(BUG 817828)`

Workaround: There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in FIPS mode.

5.36 Sentinel High Availability Installation in Non-FIPS Mode Displays an Error

Issue: The Sentinel High Availability installation in non-FIPS mode completes successfully but displays the following error twice:

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

`(BUG 810764)`

Workaround: There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in non-FIPS mode.

5.37 Appliance Update From Versions Prior to Sentinel 7.2 Fails in WebYaST

Issue: Appliance update from versions prior to Sentinel 7.2 fails because the vendor for the update packages has changed from Novell to NetIQ. `(BUG 780969)`

Workaround: Use the zypper command to upgrade the appliance. For more information, see Upgrading the Appliance by Using zypper in the *NetIQ Sentinel Installation and Configuration Guide*.

5.38 Issue with Sentinel Appliance Login

Issue: If you specified a $ character in the password, Sentinel stores the password differently in the database depending on where the $ is placed in the password. If the password starts with the $ special character, Sentinel stores the password with a file name. If the $ character is somewhere in the middle of the password, Sentinel truncates the password to the location of the $ character. `(BUG 734500)`

Workaround: The actual password is stored in the `home/novell/.pgpass` file. Obtain the password from this file and then log in to Sentinel. For example, if you specified the password as abc$123, the Sentinel stores the password as abc in the `.pgpass` file. You can log in to Sentinel by specifying abc as the password.

5.39 Error While Installing Correlation Rules

Issue: Solution Manager does not install correlation rules when a correlation rule with an identical name already exists on the system. A `NullPointerException` error is logged in the console. `(BUG 713962)`

Workaround: Ensure that all correlation rules have a unique name.

5.40 Sentinel Link Action Displays Incorrect Message

Issue: When you execute a Sentinel Link action from the Web Console Sentinel displays a success message even though the Sentinel Link Connector integrator test failed from the Sentinel Control Center. `(BUG 710305)`

Workaround: There is no workaround at this time.

5.41 Dashboard and Anomaly Definitions with Identical Names

Issue: When a Security Intelligence dashboard and an anomaly definition have identical names, the dashboard link is disabled on the Anomaly Details page. (BUG 715986)

Workaround: Ensure you use unique names when creating dashboards and anomaly definitions.

5.42 Active Search Jobs Duration and Accessed Columns Inaccuracies

Issue: The Sentinel Web Console displays negative numbers in the Active Search Job Duration and Accessed columns when the Sentinel Web Console computer clock is behind the Sentinel server clock. For example, the Duration and Accessed columns display negative numbers when the Sentinel Web Console clock is set to 1:30 PM and the Sentinel server clock is set to 2:30 PM. (BUG 719875)

Workaround: Ensure the time on the computer you use to access the Sentinel Web Console is the same as or later than the time on the Sentinel server computer.

5.43 IssueSAMLToken Audit Event Displays Incorrect Information in the Security Intelligence Dashboard

Issue: When you log in to the security dashboard and perform a search for `IssueSAMLToken` audit event, the `IssueSAMLToken` audit event displays incorrect hostname (InitiatorUserName) or (IP address) SourceIP. (BUG 870609)

Workaround: There is no workaround at this time.

5.44 Sentinel Control Center Does Not Launch When NetIQ Identity Manager Designer is Installed on the Client Computer

Issue: Sentinel Control Center does not launch when the NetIQ Identity Manager Designer is installed on the client computer and Designer uses the system JRE. Designer needs to add some supporting jar files like `xml-apis.jar` to the `lib/endorsed` directory. Some of the classes in the `xml-apis.jar` file override the corresponding classes in the system JRE that is used by the Sentinel Control Center. (BUG 888085)

Workaround: Configure Designer to use its own JRE.

5.45 Sentinel Agent Manager Does Not Capture the Windows Insertion String Fields With Null Values

Issue: While collecting event data, Sentinel Agent Manager does not capture the Windows Insertion String fields with null values. (BUG 838825)

Workaround: There is no workaround at this time.

6 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website.

For general corporate and product information, see the NetIQ Corporate website.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

7 Legal Notice

NetIQ Sentinel is protected by United States Patent No(s): 05829001.